

と、

(e) 前記セルラー・ネットワークからのデータ暗号化値の前記現在の組を前記移動局に対して送信するステップとをさらに含むプロセス。

7. 請求項6に記載のプロセスにおいて、

ステップ(e)において選択された前記データ暗号化値の現在の組に基づいて部分キーYを生成するステップをさらに含み、

ステップ(e)は、前記セルラー・ネットワークからの前記部分キーYを前記移動局に対して送信するステップを含むプロセス。

8. 請求項6に記載のプロセスにおいて、

(f) 前記現在のデータ暗号化値の組を前記移動局において前記セルラー・ネットワークから受信するステップと、

(g) 前記移動局において秘密の値xを生成するステップと、

(h) 前記移動局における前記秘密の値xに基づいて部分キーXを生成するステップと、

(i) 前記移動局からの前記部分キーXを前記セルラー・ネットワークに対して送信するステップとをさらに含むプロセス。

9. 請求項8に記載のプロセスにおいて、

(j) 前記秘密のキーxおよび前記データ暗号化値の現在の組に

基づいて前記移動局においてAキーを生成するステップをさらに含むプロセス。

10. 請求項9に記載のプロセスにおいて、

(k) 前記部分キーXを前記セルラー・ネットワークにおいて受信するステップと、

(l) 前記部分キーXと前記データ暗号化値の現在の組に基づいて、前記セルラー・ネットワークにおいてAキーを生成するステップとをさらに含むプロセス。

11. 請求項10に記載のプロセスにおいて、

(m) 前記移動局における前記Aキーを前記セルラー・ネットワークにおけるAキーと比較するステップをさらに含むプロセス。

12. 請求項10に記載のプロセスにおいて、前記移動局はメモリを含み、そして前記Aキーは前記移動局の中の前記メモリの中および前記セルラー・ネットワークの中の前記データベースの中に、前記移動局の前記セルラー・ネットワークに対するそれ以降の認証のために格納されるようになっているプロセス。

13. 請求項8に記載のプロセスにおいて、前記データ暗号化値の現在の組が、前記移動局が前記セルラー・ネットワークに対して認証された後、前記データベースから消去されるようになっているプロセス。

14. ディフィイー・ヘルマンのデータ暗号化値をあらかじめ計算するための装置であって、

ソフトウェアの命令を実行し、ディフィイー・ヘルマンのデータ暗号化値を、前記データ暗号化値に対する要求を受信する前に生成するプロセッサと、

前記ディフィイー・ヘルマンのデータ暗号化値を格納するために前記プロセッサに対して結合されているデータベースとを含む装置。

15. 請求項14に記載の装置において、Aキーに基づいてデータを暗号化するために、前記プロセッサに結合されている符号化ブロックをさらに含む装置。

16. 請求項14に記載の装置において、前記ディフィイー・ヘルマンのデータ暗号化値を移動局に対して送信するために、前記マイクロプロセッサに対して結合されていて、無線周波数を備えている基地局をさらに含む装置。

)の方法として知られている、移動局とセルラー・ネットワークの両方においてAキーを発生するための安全な方法を使用する。

OATSのプロセスは移動局にいるユーザからセルラー・ネットワークのための顧客サービス担当者に対しての電話呼出しから開始される。ユーザの呼出しに答えて、セルラー・ネットワークにおける認証センターがディフィー・ヘルマンの暗号化値を生成することを開始する。そのデータ暗号化の値は厳密な統計的条件のために、そのユーザが顧客サービス担当者と一緒に電話がつながっているままの状態で、生成するのに数分かかる。ディフィー・ヘルマンのデータ暗号化値の発生を待っていることはユーザにとって不便であり、新しいユーザを活性化するためのセルラー・ネットワークの能力を阻害する。

発明の概要

本発明は、以降の伝送のための複数のディフィー・ヘルマンのデータ暗号化値を生成するための方法を提供する。一組のデータ暗号化値が、そのデータ暗号化値に対する要求を受信する前に生成される。そのデータ暗号化値は、パブリック・モジュラス値N、秘密

キーYおよびプリミティブ要素gから構成されるグループから少なくとも1つの値を含む。そのデータ暗号化値は次にデータベースの中に格納される。その生成および格納のステップを繰り返して、データベースの中にデータ暗号化値の格納されたテールを作成することができる。

このプロセスは、無線による活性化を実装するためにセルラー・ネットワークにおいて使われる。新しいユーザが1つの移動局を活性化するために呼び出すと、セルラー・ネットワークは、既に利用可能なあらかじめ計算済みのディフィー・ヘルマンのデータ暗号化値の中から選択し、その値を移動局に対して直ちに送信することができる。このプロセスによって活性化のために必要な時間が大幅に削減され、したがって、新しいユーザおよびセルラー・ネットワークのプロバビリティにおける負担が削減される。

図面の簡単な説明

これらおよび他の目的、特徴、および利点は以下の添付図面を参照することに

【発明の詳細な説明】

改良形暗号化キーの生成

発明の分野

本発明は、データの暗号化技術に関し、特にセルラー・ネットワーク上の新しい移動局の活性化において使われるデータの暗号化の値を生成するためのプロセスに関する。

発明の背景

セルラー電話機またはセルラー・ネットワークに対して、移動局において新しいユーザを活性化するためのシステムが時によって使われてきた。その活性化のプロセスはセルラー・ネットワーク上に顧客の料金請求情報を格納し、そして移動局およびセルラー・ネットワークの両方において共有される秘密のデータを格納することを含む。その共有される秘密のデータはその移動局の電話番号、その製造者を識別するための情報およびその移動局のシリアル番号、およびその移動局とセルラー・ネットワークとの間で送信されるデータを暗号化するために使われる認証キー(Aキー)を含む。暗号化されたデータは音声およびデータの両方を含むことができる。

移動局とセルラー・ネットワークにおいて共有される秘密のデータが存在することによって、その移動局のそれ以降において使われるセルラー・ネットワークに対する認証のために、高度化された双方向の検証技法を実装することができる。その双方向の検証技法は、セルラー・ネットワークに対して許可されていないアクセスを得て、許可されている加入者に対して料金が不正に請求されるようにする目的での、無線周波(RF)の盗聴の陰謀を制限するのに役立つ。

セルラー・ネットワークに対して移動局を活性化するためのよく知られている方法は、無線による活性化遠隔サービス(over-the-air activation tele service)(OATS)であり、米国電気通信協会(Telecommunication Industries Association)(TIA)の標準ドキュメント番号:IS 136の中で記述されている。OATSはディフィー・ヘルマン(Diffie-Hellman

よって、より完全に理解される。

図1は、広く知られていて使われているセルラー・ネットワークの構成および移動局との対話のブロック図である。

図2は、移動局、基地局および認証センターの実施形態のブロック図である。

図3は、OATSのためのディフィー・ヘルマンの暗号化パラメータを生成する従来技術の方法のプロローチャートである。

図4は、OATSに対するディフィー・ヘルマンの暗号化パラメータを独立に生成することを示している本発明の方法のプロローチャートである。

発明の詳細な説明

図1は、広く知られていて使用されているセルラー・ネットワークの構成および、その移動局10との対話のブロック図を示している。セルラー・ネットワーク12は移動交換センター14を備え、それは他の移動交換センター14（図示せず）と結合することができ、そして1つまたはそれ以上の基地局16に対しても結合され、そしてホーム・ロケーション・レジスタ18、顧客サービス・センター20、認証センター22、公衆電話網（PSTN）24および統合サービスデジタル通信網（ISDN）26を備えている。

1つまたはそれ以上の移動局10が基地局16に対して信号を送信し、基地局16から信号を受信することによって、セルラー・ネットワークと対話する。移動局10が使用されているとき、それは現在の基地局16（通常は、その移動局10に最も近い基地局）に対して信号を送信し、その基地局から信号を受信する。移動局10が現在の基地局16から遠ざかるとき、現在の基地局16は、その移動局10をその移動局10に最も近くなっている別の基地局16に対して「ハンド・オフ」することができる。

移動交換センター14は、移動局から発信され、そして移動局10においてターミネートしている呼出しを、他の移動交換センター14に対して、PSTN24に対して、そしてISDN26に対して切り換える。ホーム・ロケーション・レジスタ18は移動局10を識別し、そしてその移動局10が現在存在している、あるいは普通に存在している地域の部分を示す。認証センター22は、各移

動局10とセルラー・ネットワーク12との間で送信を暗号化する目的のために、各移動局10に関連付けられているAキー

を管理する。さらに、移動局10の活性化時に、認証センター22は、移動局10に対する送信のためのデータ暗号化値を生成することができ、そしてそれ以降での送信に使われるためのAキーを生成する目的のために、移動局10から受信されたデータ暗号化値を処理する。

図2は、移動局10、認証センター22、およびセルラー・ネットワーク12の基地局16の略図を示し、新しい移動局10の活性化を実行するために使われる実施形態を示している。移動局10はメモリ30に結合されているマイクロプロセッサ28、データの入力および出力（I/O）のソース32、無線周波（RF）段34および符号化ブロック36を備えている。移動局10におけるマイクロプロセッサ28は、他の機能ブロックと対話し、データを処理し、そして移動局10を動作させるソフトウェア・プログラムの命令を実行する。また、移動局10におけるマイクロプロセッサ28は、活性化およびデータ暗号化のプロセスにおいて使われる乱数およびデータ暗号化値も発生する。メモリ30は、ランダム・アクセス・メモリ（RAM）、読み出し専用メモリ（ROM）およびプログラム可能な読み出し専用メモリ（PROM）を含むことができる。ROMまたはPROMは、その移動局の製造者およびシリアル番号を識別するための情報、その移動局の電話番号、およびその移動局のAキーなどのその移動局に関するデータを永久的に格納するために使うことができる。データの入力および出力のソース36によって、音声および他のデータを受信および送信すること以外に、ユーザは呼出しを掛け、その電話呼出しの伝送に関するメッセージを受信することができる。符号化ブロック36はデータの暗号化を実行

する。無線周波段34は移動局10からデータを受信し、移動局10に対して信号を送信する。

認証センター22の単純化された実施形態も図2に示されている。また、セルラー・ネットワーク12の基地局16も無線周波段37を備え、それは移動局1

0からデータを受信し、そして移動局10へデータを送信する。基地局16の無線周波数37は認証センター22に結合され、認証センター22は、マイクロプロセッサ38、メモリ40、符号化ブロック42、データベース44、およびデータの入力および出力(I/O)のソース46を含む。無線周波数37は、認証センター22に対して直接に接続されていくともよく、有線ネットワーク、別の無線周波数を通じて、別のセルラー・ネットワーク・コンポーネントを通じて、あるいはそれらの任意の組合せを通じて認証センター22に対して結合することができ。

マイクロプロセッサ38は、認証センター22が他の機能ブロックおよび移動局10と対話し、そしてセルラー・ネットワーク12によって要求されるように動作することができるようにするプログラム命令を実行し、そしてデータを処理する。認証センター22にあるマイクロプロセッサ38は、セルラー・ネットワーク12上で移動局の活性化のために必要なディフィー・ヘルマンのデータ暗号化値も生成することができる。メモリ40は、マイクロプロセッサ38によって必要とされるデータを格納するために使われる。符号化ブロック42は、認証センター22と移動局10との間で送信されるデータを暗号化するために使われる。データベース44は、加入者を認証して活性化するプロセスにおいて使われる情報、たとえば、1つまたはそれ以上の移動局10の電話番号、移動

局10の製造者およびシリアル番号を識別するための情報、および移動局10に関連付けられているAキーなどの情報を格納するためのデータベースである。また、データベース44は、ディフィー・ヘルマンのデータ暗号化値のテーブルを格納するためにも使うことができ、その値は移動局10をセルラー・ネットワーク12に対して活性化する際に使われる。データの入力および出力のソース46によって、認証センター22はセルラー・ネットワーク12の他の部分と対話することができ、そしてまた、認証センター22の動作について人間の対話を行うこともできるようにする。

図3は、ディフィー・ヘルマンの方法を使っているセルラー・ネットワーク12上での移動局10の活性化のための従来技術の方法を示している。ステップ5

0において、認証センター22は移動局10からの活性化のための要求を待つ。要求が受信されると、認証センター22のマイクロプロセッサ28が、ステップ52においてディフィー・ヘルマンのデータ暗号化値の生成を開始する。

ディフィー・ヘルマンのデータ暗号化値の生成は、特定の、そして厳格な規則に従って行われるので時間が掛かる。広く使われている実施形態においては、認証センター22は、秘密のキー y および公開のモジュラス N およびプリミティブ要素 g を生成しなければならない。

秘密のキー y に対する統計的な必要条件は、それが次の統計的性質を持つ160ビットの乱数であることである。 y は4より小さくなくてはならない；生成されるすべての y の値は、その統計的な分布がそれらの範囲にわたって一様でなければならない；生成されるすべての y は、同じまたは異なる移動局10に対して生成される秘密

キーとは統計的に無相関でなければならない；異なる秘密キーに対して生成される数値は、以前に使用された数値および/または移動局の指示子の値から導くことができるようなものであってはならない；異なる認証センター22によって生成される数値は、統計的に無相関でなければならない；そして認証センター22は、その秘密キー y をこの乱数の値に設定しなければならない。

公開モジュラス N は、大きな素数でなければならない。公開モジュラス N は、TIA標準IS-136に規定されているように、少なくとも768ビットの素数であって最大が1024ビットであり、次の統計的性質を有している。 N は異なる移動局に対して異なっていないなければならない； N のすべての値の統計的分布はそれらの範囲にわたって一様でなければならない； N のすべての値は同じか、あるいは異なる移動局10に対する N の他の値とは統計的に無相関でなければならない； N に対する異なる値は任意の以前に使用された数値および/または移動局の指示子の値から導くことができるものであってはならない；異なる認証センター22によって生成される数値は統計的に無相関でなければならない； $(N-1)/2$ は大きな素数の因数を有していなければならない；そして N の最上位ビットは「1」に等しくなければならない。

公開モジュラスN、秘密のキーyおよびプリミティブ要素gを生成した後、マイクログプロセッサ38は次に次の式に基づいて部分キーYを生成しなければならない。

$$Y = g^y \bmod N \quad (\text{式1})$$

次に、ステップ54において、認証センター22は公開モジュラスN、プリミティブ要素gおよび部分キーYを移動局10に対して基

地局16の無線周波数37経由で送信する。

移動局10は、N、g、およびYをステップ56において受信し、そしてステップ58において移動局10は、マイクログプロセッサ段28を使って乱数を発生し、その乱数が秘密のキーxとなる。次に、移動局10はステップ60において次の式を使って部分キーXを計算する。

$$X = g^x \bmod N \quad (\text{式2})$$

次に、移動局10は、ステップ62においてセルラー・ネットワーク12に対して移動局10の無線周波数経由でXの値を送信する。次に、ステップ64においてセルラー・ネットワーク12は部分キーXを受信する。ステップ66において、移動局10および認証センター22は両方ともAキーを以下の式に基づいて計算する。

$$A_{\text{キー}us} = (Y^x \bmod N = (g^y \bmod N)^x \bmod N) \quad (\text{式3})$$

$$A_{\text{キー}us} = (X^y \bmod N = (g^x \bmod N)^y \bmod N) \quad (\text{式4})$$

次に、Aキーがセルラー・ネットワーク12上および移動局10上で格納され、セルラー・ネットワーク12と移動局10との間のそれ以降の送信における暗号化のベースとなる。

図4は、ディフィー・ヘルマンのデータ暗号化値の生成に関連する遅延をなくする本発明の方法を示している。移動局10におけるユーザが活性化のためにセルラー・ネットワーク12にコンタクトするのを待たずに、ステップ70においてマイクログプロセッサ38は、公開モジュラスN、プリミティブ要素g、および秘密のキーyを含んでいるディフィー・ヘルマンのデータ暗号化値を生成する。N、g、およびyが生成されると、それらはそれ以降の検索のために、ステップ

72においてデータベース44の中に格納される。次

に、データベース44がステップ74において一杯であった場合、あるいは認証センターによって決定されるいくつかの他の条件に達していた場合、ディフィー・ヘルマンのデータ暗号化値の生成が終了する。それ以外の場合、この方法がステップ70から始まって繰り返され、その中で認証センター22におけるマイクログプロセッサ38がディフィー・ヘルマンのデータ暗号化値の別の組を生成する。ステップ72においてこれらの値がデータベース44に格納される。

このようにして、ディフィー・ヘルマンの利用可能な組のテーブルが、移動局10において活性化時にユーザに対してそれ以降の送信のためにデータベース44上に格納される。データ暗号化値のテーブルは認証センター22における実接によって変化する可能性がある。N、g、y、およびYまたはそれらの1つまたはそれ以上の任意の組合せが有利である。本発明の1つの好適な実施形態において、格納された値のテーブルは以下のように示される。

$$\begin{array}{ccccc} N_1 & g_1 & Y_1 & & \\ N_2 & g_2 & Y_2 & & \\ N_3 & g_3 & Y_3 & & \\ N_4 & g_4 & Y_4 & & \end{array}$$

ステップ76において、認証センター22はユーザからの活性化に対する要求を待つ。ステップ76において活性化のための要求を受信すると、認証センター22はステップ78においてディフィー・ヘルマンのデータ暗号化値のデータベース44から1つの値を選択する。ディフィー・ヘルマンのデータ暗号化値の組は先入れ先出し(FIFO)のベースで、あるいは任意の他の選択方式でデータベースからランダムに選択することができる。したがって、データ

暗号化値は要求時に直ちに使える。次に、データベース44の中に格納されているディフィー・ヘルマンの値に依存して、認証センター22は追加の値を生成しておくことができる。N、g、およびYがデータベース44の中に格納されていた場合、認証センター22は追加の値を生成する必要はない。N、g、およびy

【図2】

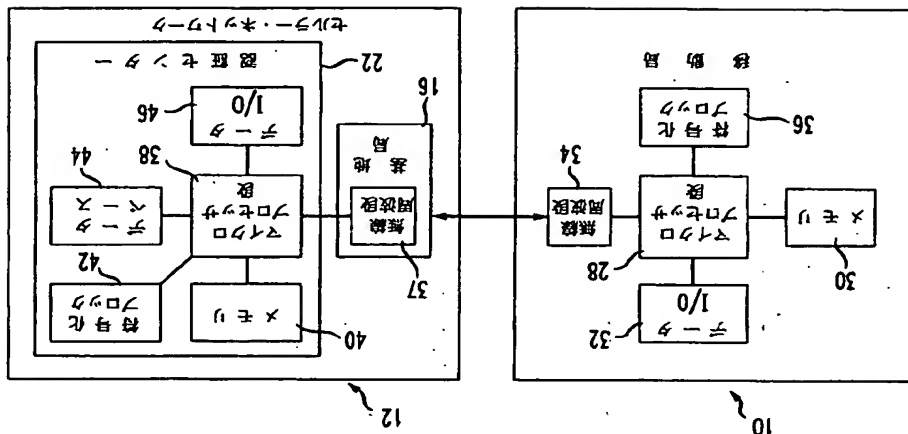
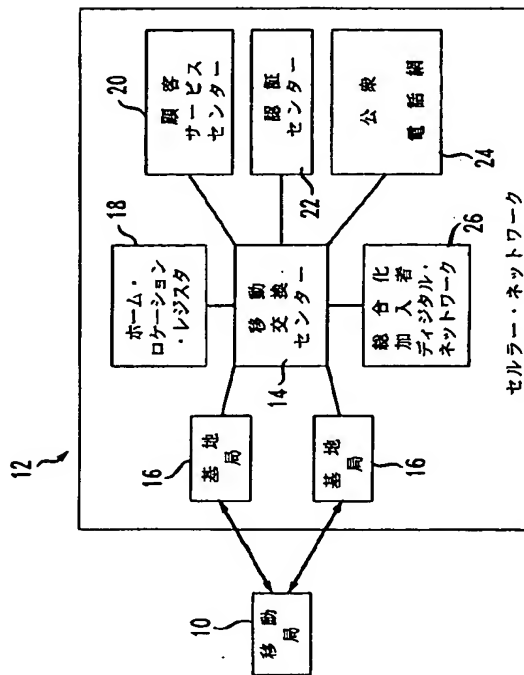


FIG. 2

が格納されていた場合、認証センターは先ず最初にYの値を上記の式1から生成しなければならぬ。N、g、またはその両方が格納されていなかった場合、その欠落している値が生成されなければならない。Yまたはyのいずれもが格納されていなかった場合、yが生成され、そしてそれから上記の式1に基づいて生成されなければならない。yが格納されているが、Yが格納されいなかった場合、Yはその格納されているyの値から上記の式1に基づいて生成されなければならない。次に、ステップ80において、データ暗号化値N、g、およびYがAキーの生成の一部として移動局に対して送信される。それ以降、図3に示されている方法のステップ56～66が実行されて活性化を達成することができる。

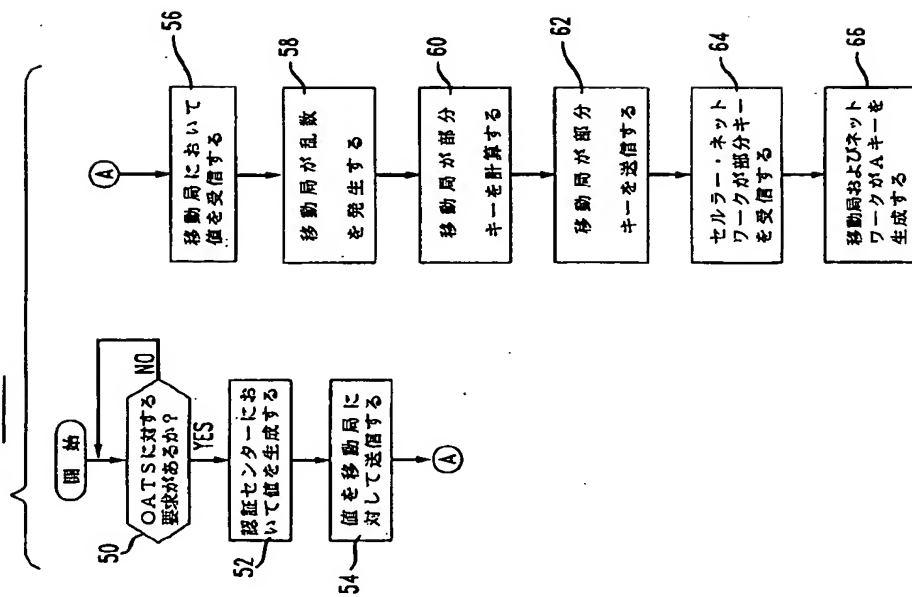
本発明の特定の実施形態が開示されてきたが、この分野の技術に熟達した人によって、それらの特定の実施形態に対して、本発明の精神および適用範囲から逸脱することなしに変更できることを理解されたい。

【図1】
FIG. 1

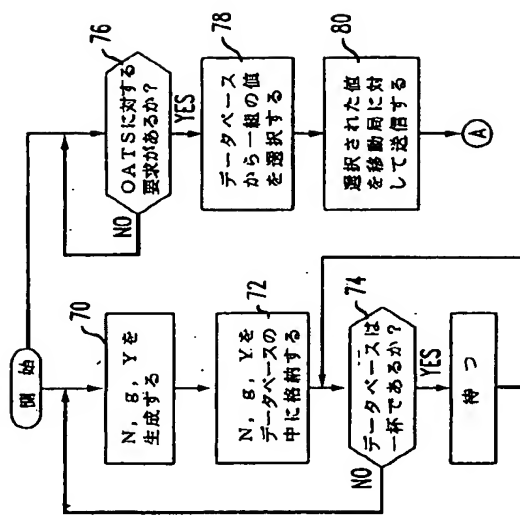


【図3】 FIG. 3

従来技術



【図4】 FIG. 4



【國際調查報告】INTERNATIONAL SEARCH REPORT

【國際調查報告】

A. CLASSIFICATION OF SUBJECT MATTER

A. CLASSIFICATION OF SUBJECT MATTER
 1.3C 6 H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED

Исправляя недостатки, мы постепенно приходим к следующему определению:

INTERNATIONAL SEARCH REPORT

International Search Report

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9628913 A	19-09-96	US 5633928 A CA 2215050 A	27-05-97 19-09-96